Method for Creating and Reading a New Certificate Types for Certification of Keys

ABSTRACT

A method for creating, storing and reading a new certificate type for certification of keys is provided. In the new certificate type, several certificates, containing a minimum quantity of redundant data fields, are collated to form one certificate and all redundant information on the certificates is eliminated. An embodiment of the new certificate type is the group certificate. The group certificate is used where several keys are to be issued at the same time for the same user by the same certification instance. By means of the group certificate, all redundant data elements are eliminated and all data elements for a set of several keys subject to certification are grouped into one certificate. This substantially reduces the memory requirement, and handling of the certificates is simplified for the communication partners. A further embodiment of the new certificate type is the basic and supplementary certificate combination. This form of certification is used where certificates are issued at different times for the same user by the same certification body. The memory requirement is consequently somewhat more than for group certificates, but greater flexibility is gained in use of the keys.